我国网站被黑情况及国内网络安全状况分析报告（修订版）

2001-05-15.12:04:49

我国网站被黑情况及国内网络安全状况分析报告

（修订版）

作者：孤独剑客

Email: janker@371.net

2001年5月15日

一、发生背景

高速发展的互联网给我们的生活、工作和人与人之间的沟通带来了极大的方便，但也成了培育黑客的温床。近年来，国际国内黑客事件的不断发生，不仅扰乱了正常的网络秩序，而且还带来了严重的经济损失，这种现象正逐步得到各个国家和政府部门的重视。特别是近来由于某些国家的强权政治和霸权主义思想有恃无恐，使得许多国家的安全和人权饱受威胁；但从长远利益考虑，国家之间近期是不可能发生战争的，但网络的无国界性给长期压抑的人们带来了发泄愤怒的机会，于是在网络上演绎了多起网络大战。其中尤其以中美大战为甚，并且随着因今年发生的中美撞机事件引发的网络黑客大战而改愈演愈烈，在5月1日左右达到高潮。初期，国外黑客PoisonBox、Prophet、Acidklown、Hackweiser和PrimeSuspectz等5个美国黑客团体对我国展开了网络攻击，后来Subex、SVUN、Hi—Tech等黑客团体也陆续加入。值得一提的是，Hi—Tech原以美国军方为入侵对象，属于技术高超的黑客组织，此次也改旗易帜，将炮口对准了中国网站。由于在技术等方面和美国的差距，使得我国在这次网络大战中损失惨重。其间，江西宜春政府网、西安信息港、贵州方志与地情网、中国青少年发展基金会网、福建外贸信息网、湖北武昌区政府信息网以及桂林图书馆、中国科学院理化技术研究所、中国科学院心理研究所等网站遭到攻击，一些大型门户网站也相继被黑。这是近年来中国网络安全受到的最大的挑战。

二、攻击特点

事情是由美国黑客先挑起来的。自4月4日以来，美国PoisonBOx、Prophet、罪恶世界、MIH等臭名昭著的黑客组织相继对中国网站发动了袭击，造成40多家网站服务一度中断，有200多家网站的页面被篡改，其中包括许多政府、企业及学校、科研机构的网站。他们声称这是一次“对中国的网络战争”，并叫嚣着：“所有的美国黑客联合起来吧！把中国服务器全都搞砸！”其中PoisonBox黑客行为最为猖獗，他们曾在最近的两周之内对域名以“.cn”结尾的部分网站进行了283次攻击。目前，PoisonBox仍在积极策划攻击行动，还不断唆使更多黑客加入战团。面对美国黑客的挑衅，中国黑客高手奋起还击，在5月1日至7日放假期间对美国网站发动了大规模的攻击行动，并在五四青年节这天达到高峰，体现了他们的爱国热忱，并以此纪念5月8日“中国驻南联盟大使馆被轰炸”这一事件。我们从这次发生的国外黑客入侵国内网站的事件上可以看出，与过去的攻击事件相比这次明显具有以下特点：

1、政治性：在被篡改的页面上留下了侮辱我国的文字和图片，是美国强权政治和霸权主义思想在网络上的真实体现。

2、挑衅性：这次网络大战的发生明显是由美国黑客组织PoisonBox最先对我国网站大肆攻击引起的，属于典型的不宣而战，符合美国人做事我行我素、缺乏道德伦理的作风。

3、目的性：主要攻击我国的政府（gov.cn）、教育（edu.cn）、科研（ac.cn）等网站为主，以破坏和扰乱我国正常的网络秩序为目的。

4、灭绝性：凡是我国的网站，无论什么性质，一旦落入美国黑客手中，就惨遭不幸，这有别于通常的黑客行为。

5、组织性：美国黑客组织严密、专业水准高而且效率明显，典型的流氓黑客军团。

6、破坏性：大多被攻破的国内网站数据被全部删除，仅保留了被更换的页面，这与通常的仅以更换页面为目的的黑客行为不同，属于极端恶劣的破坏行为。

三、攻击手法

这次发生的国外黑客入侵国内网站的事件的攻击手法，总体上说水平一般，受攻击的大多是Windows NT系统，其次是Linux、BSDI、Solaris等系统。主要是使用一些现有的工具对操作系统的弱口令或安全漏洞加以利用攻击，获得一般用户甚至管理员用户权限，进而达到实施破坏的目的。具体的攻击手法主要如下：

1、弱口令攻击：不少网站的管理员账号密码、ftp账号密码、Sql账号密码等都使用很简单的或是很容易猜测到的字母或数字，利用现有的家用PIII机器配合编写恰当的破解软件足以在短时间内轻松破解，一旦口令被破解，网站就意味着被攻破。

2、Unicode编码漏洞：对于Windows NT4.0和Windows 2000来说都存在有该漏洞，利用该漏洞远程用户可以在服务器上以匿名账号来执行程序或命令，从而轻易就可达到遍历硬盘、删除文件、更换主页和提升权限等目的，由于实施方法简单，仅仅拥有一个浏览器就可实施，所以这次被攻破的网站大多是因为存在此漏洞导致的。

3、ASP源码泄漏和MS SQL Server攻击：通过向web服务器请求精心构造的特殊的url就可以看到不应该看到的asp程序的全部或部分源代码，进而取得诸如MS SQL Server的管理员sa的密码，再利用存储过程xp_cmdshell就可远程以SYSTEM账号在服务器上任意执行程序或命令，事实上，MS SQL Server默认安装的管理员sa的密码为空，并且大多数系统管理员的确没有重新设定为新的复杂密码，这直接就留下了严重的安全隐患。

4、IIS缓冲溢出：对于IIS4.0和IIS5.0来说都存在有严重的缓冲溢出漏洞，利用该漏洞远程用户可以以具有管理员权限的SYSTEM账号在服务器上任意执行程序或命令，极具危险性。但由于操作和实施较为复杂，一般为黑客高手所用。这种攻击主要存在于Windows NT和2000系统中。

5、BIND缓冲溢出：在最新版本的Bind以前的版本中都存在有严重的缓冲溢出漏洞，可以导致远程用户直接以root权限在服务器上执行程序或命令，极具危险性。但由于操作和实施较为复杂，一般也为黑客高手所用。这种攻击主要存在于Linux、BSDI和Solaris等系统中。

6、其他攻击手法：还有利用Sendmail、Local Printer、CGI、Virus、Trojan、DOS、DDOS等漏洞攻击的手段，但在这次大战中表现的不是很明显，这里顺便提及。

四、后果分析

在已经掌握的4月份国际互联网上发生的数千起黑客事件中，针对中国大陆的就有数百起之

多，占13.82%。在所有被攻击的网站中，商业网站占54%，政府网站占12%，教育和科研网站占19%，其他类型网站占15%。据国内某知名IDC企业的技术人员介绍，他们在4月份内检测到的针对其所运营网络的扫描和探测行为达到每天8万起，实际发生的攻击数量为每天100起以上，大大超出了平时的水平。网站系统一旦遭受到攻击，数据往往被窃或删除，仅保留有被替换过的主页，导致网站形象受损并引发泄密、数据错误等问题，有的甚至整个系统被破坏，损失难以估量。在国内，除商业网站能很快恢复系统和改回被换页面外，政府、教育和科研网站大多表现迟钝，有的甚至在被黑两周后还没有恢复。目前这种攻击还在继续，它已为中国信息安全敲响警钟。信息安全关乎国家安全和主权，而我国在信息安全方面缺少人才和技术。

五、存在问题

根据国内一些网络安全研究机构的资料，国内大部分的ISP、ICP、IT公司、政府、教育和科研机构等都没有精力对网络安全进行必要的人力和物力投入；很多重要站点的管理员都是Internet的新手，一些操作系统如UNIX，在那些有经验的系统管理员的配置下尚且有缺陷，在这些新手的操作中更是漏洞百出。很多服务器至少有三种以上的漏洞可以使入侵者获取系统的最高控制权。

从以上分析来看，国内网站被黑是必然的，只是这次时间比较集中而已。从这次被攻击的网站不难看出我国的网站系统目前主要存在以下问题：

1、安全意识不强

去年10月28日，微软公司电脑系统被黑客入侵，生产软件的源代码被窃取，新开发的软件产品计划可能被盗的消息震惊了全世界。软件、网络高手如云的微软也会被“黑”？！ 我们知道，微软不是没有安装查杀木马的软件，也不是没有员工不能运行来历不明可执行程序的规定，就是因为部分主管和员工安全意识不强，违反规定才造成的，这也正是当前国际网络安全状况堪忧、危机四伏的真实写照。而针对我国网络现状而言，由于发展时间较短、基础较为薄弱，网络的安全状况就更应成为企业网络关注的重点。遗憾的是，大多企业把资金都投在了应用系统建设，却忽视了安全保障投资，殊不知一旦发生安全事件，轻则损失惨重、形象受损，重则企业倒闭破产。同国外对网络安全投资占建设总投资约20%来比，国内可怜的5%到甚至没有实在令人吃惊。

2、缺乏整体安全方案

在大多数人的眼中，在服务器前加一个防火墙就解决了安全问题，这是一种很狭隘的安全思路。防火墙仅仅是一个访问控制、内外隔离的安全设备，在底层包过滤，对付超大ICMP包、IP伪装、碎片攻击，端口控制等方面的确有着不可替代的作用，但它在应用层的控制和检测能力是很有限的，比如：这次被攻击的网站中就有不少是有防火墙的，但利用Unicode漏洞和MS SQL Server远程控制等就可轻松穿透防火墙实施攻击。另外，没有设置好密码策略、没有设置安全日志策略或没有定期分析日志发现异常现象、没有一套安全管理制度，如此等等。说到底就是缺乏一套整体安全方案，一个没有整体安全规划的系统，安全是肯定没有保障的。

3、系统本身不安全

主要是没有安全地安装配置、用户和目录权限设置及建立适当的安全策略等系统安全处理加固。例如：没有打安全补丁、安装时为方便使用简单口令而后来又不更改、没有进行适当的目录和文件权限设置、没有进行适当的用户权限设置、打开了过多的不必要的服务、没有对自己的应用系统进行安全检测等等。事实上系统和应用大多是由系统集成商来完成的，但系统集成商的做法往往是最大化安装，以方便安装调试，把整个系统调通就算完成了任务，遗憾的是留下很多的安全隐患；而安全却恰恰相反，遵循最小化原则，要求没必要的东西一定

不要，有必要的也要严加限制使用。这和系统集成好像构成了一个矛盾，事实上却不是，最小化原则实际上降低了系统负荷、提高了应用系统的性能，增强了安全性，而问题在于大多数集成商不具备专业安全设计和防范能力。

4、没有安全管理机制

安全和管理是分不开的，即便有好的安全设备和系统，没有一套好的安全管理方法并贯彻实施，值得注意的是这里强调的不仅要有安全管理方法，而且还要贯彻实施，否则安全就是空谈。相信那些被黑达两周还没有恢复的网站，要么是有安全管理制度没有执行，要么就是根本就没有安全管理制度。安全管理的目的在于两点：一是最大程度地保护网络，使得其安全地运行，再就是一旦发生黑客事件后能最大程度地挽回损失。所以建立定期的安全检测、口令管理、人员管理、策略管理、备份管理、日志管理等一系列管理方法和制度是非常必要的。

5、不理解安全是相对的

诚然，当我们的系统经过专业网络安全方案设计这一步骤，即进行了安全网络拓朴和路由、安全网络系统设计、安全产品防护、安全系统处理和整体安全检测等安全处理后，系统的安全是有保障的。但需要指出的是安全是相对的，因为随着操作系统和应用系统漏洞的不断发现以及口令很久没有更改等情况的发生，整个系统的安全性就受到了威胁，这时候若不及时进行打安全补丁或更换口令就很可能被一直在企图入侵却未能成功的黑客轻易攻破。所以，安全是相对的，是动态的，只有及时对系统安全问题进行跟踪解决，定期整体安全评估，及时发现问题并解决，才能确保系统具有良好的安全性。

6、缺少必需的安全专才

上海交通大学信息安全工程学院常务副院长李建华介绍：“我国现有信息安全专业人才仅3000人左右。”除了军队、公安部门等对高级网络安全人才需要外，政府、企业也需要信息安全方面的人才；而中国互联网本身的漏洞也急需人才来解决。显然，这样的人数与中国迅猛发展的互联网产业是不相适应的。国家有必要在大专院校设置与网络安全相关的专业，鼓励社会网络人才研究网络安全等等措施来逐步改善目前安全人才极为缺乏的状况。

六、解决之道

事实上，面对如此猖獗的黑客攻击，国内IT企业、政府、教育、科研部门没有精力也没必要对网络安全进行大量的人力和物力投入，因为社会的分工越来越细，大家只需要专注做好自己的事情，其他事情可由专业公司来完成，这样既节省了投资又能得到最好的效果，在网络安全界也一样。这方面的工作一般由安全咨询顾问公司来完成，由于网络安全涉及很多方面，包括网络设备、网络拓扑、安全产品、安全研究、漏洞解决、系统加固、系统应用、管理培训等一系列专有技术，需要投入大量的人力和物力才能做的很好，这是其他公司、企业或部门所无法替代的。诚然，在网络上也曾流行不少简单的安全处理办法，但那几乎都起不了多大作用；只有安全顾问公司，才能为您量体裁衣，制定完整的安全方案。合适的安全产品选型和部署，完善的系统加固处理，良好的安全管理培训及快速的安全事件响应，才是安全确有保障的解决之道。因此，要想很好地保护网站系统需要从以下几个方面着手：

1、成立网络安全领导小组

要从上到下把网络安全重视起来，由行政领导牵头，技术部门负责，系统和管理员参与，成立安全管理领导监督小组。加强网络安全项目的建设和管理，负责贯彻国家有关网络安全的法律、法规，落实各项网络安全措施；督促有关部门对网络用户的安全教育，监督、检查、指导网络安全工作；监督网络安全管理制度的执行和贯彻，查处违反网络安全管理的违纪、违规行为；协助、配合公安机关查处网络犯罪行为。

2、制订一套完整的安全方案

一套完整的安全方案是整个系统安全的有力保障，要结合自己实际的网络状况，从人力、物力、财力做好部署与配置，由于安全方案涉及到了安全理论、安全产品、网络技术、系统技术实现等多方面专业技能，并且要求要有较高的认知能力，大多数企业、公司、政府等可能不具备此能力，此时可以聘请专业安全顾问公司来完成，大多安全顾问公司在做安全方案方面有着丰富的经验，能够制订出符合需要的合理的安全方案来。

3、用安全产品和技术处理加固系统

说到底，要达到网络系统是安全的目的，就必须对系统进行一系列的处理，比如：安装防火墙和入侵检测系统等安全产品、为系统打补丁堵塞安全漏洞、用户和文件目录权限管理、设置安全策略等系统安全处理，以求消除隐患，加固系统。由于这种系统加固服务需要非常专业的安全技能，一般的企业和公司要想做好是不现实的，而大多安全咨询顾问公司都提供有这种服务。主要加固项目如下：

O网络拓扑路由分析

O火墙内外部隔离

O入侵检测系统跟踪

O网站恢复系统监控

O系统安全加固处理

O应用系统安全检测

O整体网络安全评估

4、制定并贯彻安全管理制度

在对系统安全方案和系统安全处理的同时，还必须制定出一套完整的安全管理制度，如：外来人员网络访问制度，服务器机房出入管理制度，管理员网络维护管理制度等等。约束普通用户等网络访问者，督促管理员很好地完成自身的工作，增强大家的网络安全意识，防止因粗心大意或不贯彻制度而导致安全事故。尤其要注意制度的监督贯彻执行，否则就形同虚设。

5、建立完善的安全保障体系

建立完善的安全保障体系是系统安全所必需的，如管理人员安全培训、可靠的数据备份、紧急事件响应措施、定期系统安全评估及更新升级系统，如此这些都为系统的安全提供了有力的保障，确保系统能一直处于最佳的安全状态，即便系统受到攻击，也能最大程度地挽回损失。

6、选择一个好的安全顾问公司

可以说，在两年前国内还没有一家具有真正意义上的网络安全顾问公司，但由于目前形势的需要，国内的安全顾问公司可以说是蓬勃发展，百花齐放，但不外主要是从以下几种转型而来的：

（1）网络安全产品公司兼做网络安全顾问服务

（2）传统系统集成公司设立网络安全顾问部门

（3）自由黑客组织转型为专业网络安全顾问公司

（4）国家科研教育机构成立的网络安全顾问公司

选择安全顾问公司是要必须非常谨慎的，要从安全公司的背景、理念、实力、管理等多方面进行考查，不仅要看一个安全公司的技术和资金实力，而且还要看公司人员的组成，因为一旦你的系统交给了安全公司，其实你的系统就等于对其百分之百的开放，但大多网络安全公司人员层次不齐，即便技术和资金很强，但若管理不善，人员流失较大，就会使得其客户的系统资料就处于不可控状态，从而带来极大的安全隐患，所以一旦选择失误，不仅不能带来安全保障，而且可能会带来无尽的梦魇。

七、作者声明

本文为作者根据自己多年的网络安全工作经验而写，属个人观点，目的是希望通过本文让大家对我国的网络安全状况有一个全面清醒的认识，也希望政府等有关部门能够及时采取措施，保护好国内的网络信息系统，确保国家的经济建设持续稳步发展。本文由孤独剑客撰写，版权归广州金华诚科技有限公司所有，由中国红客联盟发布，欢迎全文转载，但务必请著名作者、版权和出处，谢谢！

参考资料：

新浪网新闻中心 - http://dailynews.sina.com.cn

发布网站：

中国红客联盟 - http://www.cnhonker.com

联系作者：

孤独剑客个人主页 - http://janker.126.com

cnhonker.com.

>>相关资料

关闭本窗口